

BEST AVAILABLE COPY

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-121387

(43)Date of publication of application : 06.05.1997

(51)Int.Cl.

H04Q 7/38
H04Q 7/34

(21)Application number : 08-204957

(71)Applicant : NOKIA MOBILE PHONES LTD

(22)Date of filing : 02.08.1996

(72)Inventor : MECHE PAUL S
VAISANEN AHTI

(30)Priority

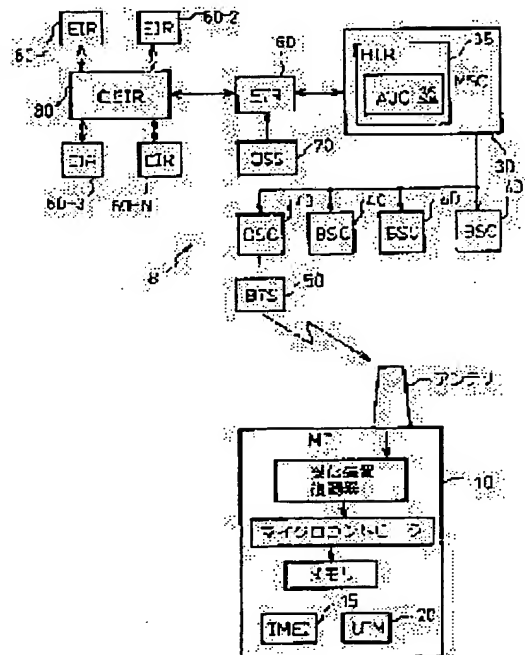
Priority number : 95 511519 Priority date : 04.08.1995 Priority country : US

(54) MOBILE COMMUNICATION NETWORK AND METHOD FOR LOCKING REMOTE MOBILE TERMINAL EQUIPMENT SELECTED FROM THE MOBILE COMMUNICATION NETWORK

(57)Abstract:

PROBLEM TO BE SOLVED: To provide the mobile means network in which a lock function of a user identification module(UIM) is automatically started by a signaling of a communication network via a common radio interface from a base station to a mobile telephone set.

SOLUTION: The communication network 8 inquires of an international mobile terminal identification(IMEI) unit 15 of a mobile telephone set 10 used by a subscriber of the system periodically or regularly. If the IMEI of the mobile telephone set is listed on a 'theft article list', the communication network communicates a message with the mobile telephone set via a radio interface and allows the mobile telephone set to start a UMI lock function 20 based on the sent bit pattern.



LEGAL STATUS

[Date of request for examination]

01.08.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(51) Int.Cl. ⁸	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 Q 7/38			H 0 4 B 7/26	1 0 9 S
7/34			H 0 4 Q 7/04	C

審査請求 未請求 請求項の数18 O L (全 12 頁)

(21) 出願番号 特願平8-204957

(22) 出願日 平成8年(1996)8月2日

(31) 優先権主張番号 5 1 1 5 1 9

(32) 優先日 1995年8月4日

(33) 優先権主張国 米国 (U S)

(71) 出願人 590005612

ノキア モービル フォーンズ リミティ
ド

フィンランド国、エフアイエヌ-24101

サロ、ビー、オー、ボックス 86、ナコラ
ンカツ 8

(72) 発明者 ボール エス、メシエ

アメリカ合衆国、テキサス 75082、リチ
ャードソン、スプリング レイク ドライ
ブ 2618

(72) 発明者 アーティ パイサネン

アメリカ合衆国、カリフォルニア 92014、
デルマー、マンゴー ドライブ 13353

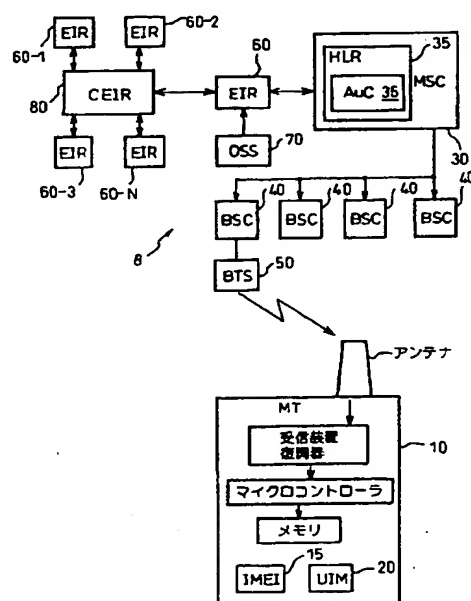
(74) 代理人 弁理士 石田 敬 (外3名)

(54) 【発明の名称】 移動通信網及び該移動通信網の選択された遠隔移動端末装置をロックする方法

(57) 【要約】

【課題】 基地局から移動電話への共通無線インターフェースを介する当該通信網のシグナリングによってユーザー識別モジュール (UIM) のロック機能が自動的に起動されるようになっている移動通信網を提供することを目的とする。

【解決手段】 該通信網は、該システムで加入者が使っている移動電話の国際移動端末装置識別 (IMEI) ユニットを定期的に又は規則的に問い合わせる。もし移動電話の IMEI が「盗品リスト」に載っていたならば、該通信網は、無線インターフェースを介して該移動電話とメッセージをやりとりして、送ったビットパターンにより該移動局に UIM ロック機能を起動するように指令する。



【特許請求の範囲】

【請求項1】 少なくとも1つの中央基地交換網と、電子信号を送受信するための回路を内蔵する複数の遠隔移動端末装置とから成る移動通信網において、前記遠隔移動端末装置の各々は、該装置からの送信を制御するための特定のユーザー専用のデータを内蔵するユーザー識別モジュール(UIM)を含んでおり、

前記中央基地交換網は、選択された遠隔移動端末装置にデータ信号を送って前記の選択された遠隔移動端末装置を前記の含まれているUIMに選択的にロックするとともに前記の含まれているUIMを前記の選択された遠隔移動端末装置にロックするための手段を含んでおり、これにより前記の選択された遠隔移動端末装置の他の前記UIMでの動作を選択的に阻止するとともに前記の含まれているUIMの他の前記遠隔移動端末装置での動作を阻止することを特徴とする移動通信網。

【請求項2】 前記中央基地交換網は、選択された遠隔移動端末装置にデータ信号を送って前記の選択された遠隔移動端末装置を前記の含まれているUIMにロックすることにより前記の選択された遠隔移動端末装置の他の前記UIMでの動作を阻止するための手段を有する、請求項1に記載の移動通信網。

【請求項3】 前記中央基地交換網は、選択された遠隔移動端末装置にデータ信号を送って前記の含まれているUIMを前記の選択された遠隔移動端末装置にロックすることにより前記の含まれているUIMの他の前記遠隔移動端末装置での動作を阻止するための手段を有する、請求項1に記載の移動通信網。

【請求項4】 前記遠隔移動端末装置の各々の各UIMは前記の特定のユーザー専用のデータを記憶するための記憶手段を含んでいる、請求項1に記載の移動通信網。

【請求項5】 前記遠隔移動端末装置の各々の各UIMは、前記中央基地交換網から送られた前記データ信号に応答して、その送られたデータ信号のデータが前記遠隔移動端末装置の前記UIMに記憶されている前記の特定のユーザー専用のデータと同一であるときには前記遠隔移動端末装置の他のUIMでの動作を阻止するための手段を含む、請求項1に記載の移動通信網。

【請求項6】 前記遠隔移動端末装置はセルラー電話である、請求項1に記載の移動通信網。

【請求項7】 前記遠隔移動端末装置の各々は独特の国際移動端末装置識別(IMEI)ユニットを含む、請求項1に記載の移動通信網。

【請求項8】 前記中央基地交換網は、少なくとも1つの基地局コントローラ(BSC)と、前記データ信号を前記の選択された遠隔移動端末装置に送るための少なくとも1つの基地局送受信システム(BTS)とに接続された移動交換センター(MSC)を含む移動交換網を含む、請求項1に記載の移動通信網。

【請求項9】 前記移動交換センター(MSC)は、真

実性の確認センター(AUC)を有するホームロケーション・レジスタ(HLR)を含んでおり、前記移動交換センター(MSC)は、前記移動端末装置の正当性及び状況に関するデータを内蔵する装置識別レジスタ(EIR)に接続されている、請求項8に記載の移動通信網。

【請求項10】 少なくとも1つの中央基地交換網と、電子信号を送受信するための回路を内蔵する複数の遠隔移動端末装置とを有する移動通信網の選択された遠隔移動端末装置をロックする方法において、前記遠隔移動端末装置の各々は、該装置からの送信を制御するための特定のユーザー専用のデータを内蔵するユーザー識別モジュール(UIM)を含んでおり、この方法は、前記中央基地交換網から選択された遠隔移動端末装置のUIMへデータ信号を送るステップ(ステップ1)と、前記中央基地交換網から送られた前記データ信号を受け取って前記の選択された遠隔移動端末装置を前記の含まれているUIMに選択的にロックし且つ前記の含まれているUIMを前記の選択された遠隔移動端末装置にロックすることにより、前記の選択された遠隔移動端末装置の他のUIMでの動作を阻止するとともに前記の含まれているUIMの他の前記遠隔移動端末装置での動作を阻止するステップ(ステップ2)とから成ることを特徴とする方法。

【請求項11】 前記の含まれているUIMは前記の特定の遠隔移動端末装置にロックされる、請求項10に記載の移動通信網の選択された遠隔移動端末装置をロックする方法。

【請求項12】 前記のステップ2において前記の特定の遠隔移動端末装置は前記の含まれているUIMにロックされる、請求項10に記載の移動通信網の選択された遠隔移動端末装置をロックする方法。

【請求項13】 前記のステップ2は、前記UIMの前記の特定ユーザー専用データを前記中央基地交換網から受け取ったデータ信号と比較し、前記UIMをロックし、前記の受け取ったデータが前記の特定ユーザー専用データと同一であるときには前記の選択された遠隔移動端末装置の動作を阻止することを含む、請求項10に記載の移動通信網の選択された遠隔移動端末装置をロックする方法。

【請求項14】 前記UIMに内蔵された真実性の確認手続きを更に含んでおり、前記のステップ2は前記真実性の確認手続きの結果を比較することを更に含む、請求項13に記載の移動通信網の選択された遠隔移動端末装置をロックする方法。

【請求項15】 前記のステップ1は、前記の選択された移動端末装置の国際移動端末装置識別(IMEI)情報を得、国際移動端末装置識別情報の状況に関して装置識別レジスタ(EIR)に問い合わせ、その選択された遠隔移動端末装置が盗まれているか否か判定し、ユーザー識別モジュールロックコマンドを前記の選択された

遠隔移動端末装置に送るステップを更に含む、請求項10に記載の移動通信網の選択された遠隔移動端末装置をロックする方法。

【請求項16】 選択された遠隔移動端末装置の前記UIMに内蔵されている真実性の確認手続きを更に含んでおり、前記のステップ2は前記真実性の確認手続きの結果を比較することを更に含む、請求項15に記載の移動通信網の選択された遠隔移動端末装置をロックする方法。

【請求項17】 前記のステップ2は前記中央基地交換網から送信された受信コマンドがロックコマンドであるか否か判定し、前記ロックコマンドの真実性を確かめ、移動端末装置のユーザー識別モジュールへのロックを実行するステップを含む、請求項10に記載の移動通信網の選択された遠隔移動端末装置をロックする方法。

【請求項18】 前記のステップ2は、前記の選択された遠隔移動端末装置がロックされたという肯定応答を前記の選択された遠隔移動端末装置から前記中央基地交換網へ送るステップを更に含む、請求項17に記載の移動通信網の選択された遠隔移動端末装置をロックする方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、例えば携帯電話などの通信用移動端末装置と、その様な端末装置を利用する通信網とに関する。本発明は、特に、ユーザー識別モジュール(UIM)を採用する携帯電話に関する。

【0002】

【従来の技術】電話を手操作でユーザー識別モジュール(UIM)にロックすることのできる加入者又はユーザー識別装置を持った携帯電話システムが知られている。

【0003】1993年3月29日に出願された「移動端末装置の加入者識別モジュールを遠隔操作で更新する機能を持った移動通信網」という題名の、グリーン(Green)の欧州特許出願第93302420、0号(公報第0562890A1号)は、無線電話で移動電話と通信をする移動交換センターを含む交換網を有する通信網を開示している。その移動装置は、移動装置の動作と、移動装置のユーザーが利用し得る設備とを制御するためのデータを記憶する加入者識別モジュールを内蔵している。交換網は、加入者識別モジュールに記憶されているデータを変更し、従って、利用可能な設備での動作を変更する更新信号を移動装置に送る。

【0004】前記の出願は、無線でUIMをプログラミングする技術を開示しているが、公報第0562890A1に記載されているように電話をプログラミングする方法や技術を開示していない。

【0005】

【発明が解決しようとする課題】目下、特にGSM(the Groupe Speciale Mobile)規格に基づく移動電話は、

以前は加入者識別モジュール又はSIMと称せられ、現在はユーザー識別モジュール(UIM)と称せられている電子モジュールを内蔵している。このUIMは移動電話(本明細書では移動端末装置(MTと略記)とも称する)により使用されるべきデータを記憶する。UIMは、特定のユーザーのための独自の識別子を持つように予め構成されるとともに、適当な真実性の確認機能を持つこともできる。UIMは、ページングメッセージや電話番号簿などの暫定的データを記憶することもできる。

【0006】現在のGSMに基づくシステムでは、加入者識別は移動端末装置(MT)には関連していない。それは、UIMのユーザーによりなされる。UIMは、電話に取り付けられるようになっていて独自のユーザー識別情報を有するモジュール或いはスマートなカードである。

【0007】GSMに基づくシステムでは、ユーザーは自分のUIMカードをどの移動端末装置にも挿入することができ、使用されているその特定の端末装置に付随する情報ではなくてそのUIM上の情報を介してGSM通信網により認識される。このシステムでは、移動端末装置はIMEI(International Mobile Equipment Identity(国際移動端末装置識別)情報)により識別可能である。しかし、この情報をチェックするための照会は、処理に関して「費用がかかり」、通常は毎呼には確認されない。

【0008】これらの要素を、GSMに基づくインターフェースを使用する端末装置の広大な「ブラックマーケット」を開拓した泥棒達が活用して、数十万台もの移動端末装置が毎年盗まれるという結果を招いている。

【0009】

【課題を解決するための手段】本発明は、盗まれた移動端末装置を発見したならば、その移動端末装置を、その移動端末装置で使用されているUIMカードに直ちに「ロック」することによって、その盗まれた移動端末装置の価値を低下させるものである。移動端末装置を特定のUIMにロックするということは、その移動端末装置を他のUIMで使うことができなくなることとを意味し、従ってその再販価格を低下させる。また、この操作に加えて、関係当局によるその移動端末装置の取り戻しのための追跡調査のために、盗まれた移動端末装置に使われているUIMに関する情報収集を行う。

【0010】一般に、ロック機能は4～8桁のピンコードを有し、起動される場合には、移動端末装置がパワーアップされる毎に、いずれかの操作が行われる前に、入力されなければならない。

【0011】また、移動端末装置は、マスターパスワード無しでは無許可のUIMを移動端末装置が受け入れるのを阻止する様に設計されたUIMロックも提供する。起動されると、移動局は前に許可されたUIMだけを受け入れる。

【0012】本発明の目的は、UIMのロックとロック解除とがBTSと移動局との共通無線インターフェース経由のシグナリングを介して通信網により自動的に起動されるようになっている移動電話システムを提供することである。

【0013】本発明の他の目的は、UIMを、それと関連する特別の移動電話にのみ使用し得るようにUIMをその移動電話に随意にロックすることができるようになっている移動電話システムを提供することである。

【0014】本発明の他の目的は、移動電話を特別のUIMにのみ使用し得るように移動電話をそのUIMに随意にロックすることができるようになっている移動電話システムを提供することである。

【0015】本発明の他の特徴、長所及び利益は、添付図面と関連させて以下の記述を考慮することから明かとなろう。如上の一般的記述と以下の記述は例示的な説明をするものであって、本発明を限定するものではないことが理解されなければならない。本発明に組み込まれて本発明の一部を構成する添付図面は、明細書とともに、本発明の原理を一般的用語で説明するのに役立つものである。明細書及び図面の全体にわたって同じ数字は同じ部分を指している。

【0016】

【発明の実施の形態】現在、GSM移動端末装置は、もし正当な所有者が自分の移動端末装置を自分のUIMに「ロック」することを忘れたり無視したりした場合に、盗難後に単に有効なUIMカードを挿入するだけで簡単に再使用される。また、賃貸ユニットは通常は特別のUIMカードにロックされていないので、賃貸の移動端末装置は特に窃盗に対して弱い。このような事情があるために盗まれたGSM移動端末装置の繁盛している市場がある。本発明は、盗品であると判定された移動端末装置を該移動端末装置に挿入されているUIMにロックすることにより再販売に関しての価値を低下させることのできるメカニズム及び方法を定義する。

【0017】本発明の移動端末装置(MT)は、無線でのコマンド(over-the-air command)によりUIMにロックされる。また、本発明は、移動端末装置に挿入されたUIMをその移動端末装置のIMEIにロックすることによって、そのUIMを、該UIMがロックされた移動端末装置においてのみ使用し得るようにすることのできるシステムを提供する。

【0018】詳しく述べると、電話通信網は、該システムで加入者が使っている移動端末装置のIMEIに定期的に又は規則的に照会をする。もし移動端末装置のIMEIが「盗品リスト」に載っているのが分かったならば、通信網は無線インターフェースを介して送信したビットパターンを用いてUIMロック機能を起動するべき旨のメッセージを該移動端末装置とやりとりすることにより該移動端末装置にUIMロック機能を起動するよう

に指令する。

【0019】通信網は、通常、例えば無線電話等により移動電話等の移動端末装置(MT)と通信をする移動交換センター(MSC)を含む。移動端末装置は、該移動端末装置の動作と、そのユーザーが利用することのできる設備とを制御するためのデータを記憶する加入者(又はユーザー)識別モジュールを内蔵する。

【0020】本発明によると、交換網は、移動端末装置のデータ及び保障状況及び/又はユーザー識別モジュールの保障状況を変更する更新信号を移動端末装置に送る。

【0021】図1に通信網が示されており、この通信網は移動電話等の移動端末装置(MT)10と交換網8とを含む。交換網8は、移動交換センター(MSC)30と、移動端末装置10がその中で動作することのできる種々のセルサイトのための複数個の基地局コントローラ(BSC)40とを含む。装置識別レジスタ(EIR)60は共通装置識別レジスタ(CEIR)80に接続されており、このCEIR80は他の交換網とそれに関連する移動端末装置とに関連する他の装置識別レジスタ60-1、60-2、...60-Nに接続されることが出来る。装置識別レジスタ60を更新するためのオペレーションサブシステム(OSS)70を設けることができる。移動端末装置10等の移動端末装置との無線での通信は基地局送受信ユニット(BTS)50を介して行われる。

【0022】通信網の移動端末装置10等の各端末装置は、特定のユーザーのための独特の予めプログラムされたデータを記憶するユーザー識別モジュール(UIM)20と、国際移動端末装置識別(IMEI)ユニット15とを有する。各国際移動端末装置識別ユニット15は、その移動端末装置10に独特のものであって、移動交換センター30に対して移動端末装置10を特定するために使用される。

【0023】図1において、多数の基地局コントローラBSC40のうちの1つを介して、それに付随する基地局送受信システムBTS50経由でMSC30から移動電話又はその他の移動端末装置MT10へ通常の通信が通信ネットワーク間で行われる。

【0024】MT10は、ユーザー識別モジュール(UIM)20をそなえ、該モジュールは特定のユーザーの独特の識別子と、そのユーザーが利用することのできる真実性の確認機能とを記憶する。MT10は、独特の国際移動端末装置識別(IMEI)ユニット15も内蔵している。

【0025】MSC30は、特定のユーザーのためのホームロケーション・レジスタHLR35にアクセスするための通信チャネルを有する。HLR35は、ユーザーの真実性確認のために使われる保障データを管理する真実性確認センターAuC36と呼ばれる機能部分を含ん

でいる。HLR35のAuC36の機能と、UIM20の対応する真実性確認機能とは、連携して、ユーザーを確認することにより種々の不正使用を防止するための比較的に確実で強固な手段を提供するものである。

【0026】MSC30は、通信網に知られている国際移動端末装置識別(IMEI)ユニット15を介して移動端末装置MT10の正当性及び状況に関する情報を内蔵するデータベースである装置識別レジスタEIR60にアクセスするための通信チャネルを有する。EIR60は3つの「リスト」を内蔵している。1つは、有効な種類承認済み移動端末装置MT10の範囲を包含する「ホワイトリスト」である。他の1つは、盗まれたか、

或いはひどく故障していると通知されているIMEI15のリストを包含する「ブラックリスト」である。第3のリストは、当局がブラックリストに載せるべきことを確かめる前の怪しい装置を含む、「ホワイト」と「ブラック」との中間の「グレイリスト」である。

【0027】本発明のプロセスのステップは図2及び図3のブロックで示されているとおりである。MT10とMSC30との間での通信の開始の際に、当業者に周知されている種々の必須のメッセージのやりとりが行われる。この在来のメッセージのやりとりの後に、MSC30は、図2のブロック300に示されているようにMT10のIMEI15を得るように求められる。在来のシステムでは、これは、MT10への識別要求メッセージ(IDENTITY REQUEST Message)の送信により達成される。在来のMT10は、IMEI15を含む識別応答メッセージ(IDENTITY RESPONSE Message)で答える。本発明の特徴の1つは、IMEI15の情報を上記した在来の必須のメッセージに含ませることによって、このメッ

セージ交換を最適化することにある。

【0028】本発明の好ましい実施例では、IMEI15の情報はMT10からの位置更新要求メッセージ(LOCATION UPDATING REQUEST Message)に含まれる。

【0029】在来のシステムにおける位置更新要求メッセージのフォーマット及び構造は、MT10がUIM20を内蔵していなかったり或いはUIM20が何らかの理由から無効であると考えられる場合には、IMEIを含むだけである。本発明の最適化の特徴の主題は、位置更新要求メッセージにTMSI又はIMS Iも含まれているか否かに関わらず、常にIMEIをこのメッセージに含ませることである。TMSI(Temporary Module Subscriber Identity)又はIMS I(International Module Subscriber Identity)も位置更新要求メッセージに含まれている場合には、このメッセージは、TMSI又はIMS Iについて1つ、及びIMEIについて1つ、合計で2つの移動端末装置識別情報(MOBILE IDENTITY information)を含まなければならない。位置更新要求メッセージがIMEIのみを含んでいる場合には、このメッセージは今日のシステムで使われている在来の位

置更新要求メッセージと同一でなければならない。

【0030】IMEI15を得る方法とは無関係に、MSC30の明示の識別要求(IDENTITY REQUEST)シーケンスを介して又は自動的に位置更新要求(LOCATION UPDATING REQUEST)の好ましい強化メッセージ(preferred enhancement)又はその他の在来の必須メッセージを介して、MSC30は、図2のブロック305において、MT10から通知されたIMEI15の状況を判定するためにEIR60に照会を行う。IMEI15が盗まれた移動電話として又はひどい故障のある装置として「ブラックリスト」に載っているとEIR60が指摘したならば、ブロック310からブロック311へ移行して、MSC30はMT-UIMロック機能が作動可能(イネーブル)になっているか否かを判定する。ブロック310においてEIR60の照会により移動端末装置が盗まれたり「ブラックリスト」に載っていたりしないことが分かったならば、ブロック335に移行してプロセスは終了する。

【0031】MT-UIMロック機能は通常は作動可能にされるけれども、特定のMSC30については、そのオペレータが希望する場合には、作動不能にされる。ブロック311でこの機能が作動可能であればブロック311での分岐は図3のブロック315へ移行する。もしMT-UIMロック機能が作動不能になっていれば、ブロック311での分岐はブロック320へ移行する。

【0032】ブロック315に至ると、MSC30は、MT-UIMロックコマンドを示す保障要求メッセージ(SEcurity REQUEST MESSAGE)(図7(A))を作成して、図1に示されているMT10と通信中のBSC40ユニット及びBTS50ユニットを介してこのメッセージを送る。本発明の好ましい実施例では、全ての保障要求メッセージは暗号モードで送られる。

【0033】MT-UIMロックコマンドを意味する保障要求メッセージ(SEcurity REQUEST MESSAGE)は、該コマンドは有効であって無許可のいたずらや「ハッキング(hacking)」の結果ではないことを保証する手段をMT10に与えるために、ユーザのUIM20に関連するHLR35のAuC36の機能を介して提供されるRAND及びSRES(真実性確認パラメータ)の対を含んでいる。ブロック315からブロック316(図4及び図5参照)へ移行する。ブロック316で、MSC30はMT10からの応答を待つ。

【0034】図4及び図5は、本発明に関連する移動端末装置MT10の論理の概要を示す。MSC30からメッセージを受け取ると、MT10は、受け取ったメッセージが新たに定義されたロックの1つを起動させるコマンドを表しているのか否かを判定しなければならない(ステップ100)。ステップ105において、そのメッセージがMT-UIMロックを意味する保障要求メッセージであるか否かを検査するチェックが第1の好まし

いチェックであるとされている。もしメッセージがそのようなコマンドを含んでいるならば、ステップ105からステップ120へ移行する。もしメッセージがMT-UIMロックでなければ、ステップ105からステップ110へ分岐する。

【0035】移動端末装置MT10のステップ110以降の処理について、図3のUIM-IMEIロックのステップ325に関連するMSC30の論理の後に、解説をする。

【0036】図4のステップ120において、MT10は、受け取ったメッセージが正当であるか否かを確かめなければならない。このことは、UIM20での在来の真実性確認手続きをMT10での新しい手続きと組み合わせて利用して該機能を実行することによって、行われる。図7(A)に記されているように、MT-UIMロックメッセージは、当業者に周知されているAuC36からのRANDを含んでいる。この手続きを強化するために、本発明の好ましい実施例は、ハッキングからの保護のために追加の要件をRANDに課す。それらの要件は、慎重に考慮されるべきであり、また特定の実施に特有のもでなければならない。好ましい強化方法は、ランダムに選ばれたRANDを伴う真実性確認要求(AUTHENTICATION REQUEST)をMT10に作成させて、その要求をMSC30に送らせることである。するとMSC30は、MT10から受け取ったRANDを適切なHLR35のAuC36の機能に送り、正しいSRES応答を受け取る。MSC30は、その後、前記SRESを含む真実性確認応答メッセージ(AUTHENTICATION RESPONSE message)を作成してMT10に送る。するとMT10は、MSC30から受け取った真実性確認応答(AUTHENTICATION RESPONSE)の中のSRESを、初めにMSC30に真実性確認要求メッセージで送られたRANDを用いてUIM20が計算したSRESと比較する。この2つのSRESの値が一致すれば、保障要求は本物である(真実性がある)と考えられる。この方法は、当業者には容易に理解できる上記のメッセージ交換を支援するようにMSC30とAuC36とを改造することを必要とする。ここで考察している強化方法の他の実例は、前に受け取ったRANDの十分な長さのリストを維持して、メッセージで受け取ったRANDをこのリストと付き合わせて検査することである。維持されているリストの中にそのRANDが見つかって、その様な一致の確率がありそうもないと人が考えたならば、そのメッセージを捨てることができ、ステップ131へ分岐をする。この種の手続きを、例えばRANDを含む種々のメッセージを受け取る頻度を監視するなどの他の手続きと組み合わせることができる。けれども、追加の強化の方法を詳しく特定することは、与えるべきでない情報を「ハッカー」に与える結果を招くだけである。特定のMT10装置のために選ばれた好ましい強化方法をRANDが承認す

ば、MT10は真実性確認プロセスを続行する。RANDは在来手段を介してUIM20に送られ、UIM20は、UIM20の真実性確認論理により在来方法で計算されたSRES値を返す。ステップ130において、MT10は、MSC30から受け取ったMT-UIMロックメッセージの中のSRESをUIM20が計算したSRESと比較する。その2つのSRESの値が同一であるならば、MT-UIMロックコマンドは本物である(真実性がある)と見なされて正当なものとして承認され、次にステップ130からステップ140へ移行する。ステップ130で本物ではない(真実性がない)と判定されたならば、ステップ131へ移行する。

【0037】ステップ140においてMT10は内面的なUIMロック手続きを実行してMT10に現在装填されているUIM20のカードのみを容認するようにMT10の処理を変更する。UIMロック手続きは当該MT10のハードウェア及びソフトウェアのデザインに独特のものであり、「ハッキング」その他の不正行為からこの機能を実際に守るために、厳重に保護されなければならない。特定のMT10のためのUIMロック手続きは当業者にはよく知られているけれども、特定のMT10のデザインへの適用は、それを開示すれば安全が損なわれる危険があるために、決して開示されない。ステップ140からステップ141へ移行し、ここでMT10はMT-UIMロック手続きが成功したか否か判定する。もし成功であればステップ142へ、失敗であればステップ131へ分岐する。

【0038】ステップ142においてMT10は、該MT10が当該UIM20にロックしていることを確認しており、従ってMT-UIMロックが成功したことを意味する保障応答(SEcurity RESPONSE)(図7(B))を作成する。このメッセージはMSC30に送られる。次にステップ150に移行してプロセスは終了する。

【0039】ステップ131は、MT-UIMロック動作が失敗したこと、及びその失敗の理由を示す保障応答を作成する。このメッセージは、MSC30に送られて、失敗の理由が真実性がなかったこと(authentication failure)なのか或いはその他の処理の失敗であるのかを指摘する。次にステップ150に移行してプロセスは終了する。

【0040】MT10の制御の流れを詳細に検討したので、次に図3のステップ316を参照するが、そこではMSC30の制御の流れに関する検討は行われていなかった。MSC30は、MT10から応答を受け取るか又はMT10からの応答を処理すると、ステップ316からステップ317へ移行し、このステップでMSC30は、将来ステップ330で参照するためにMT10からのMT-UIMロック動作の結果に関する情報を記憶する。次にステップ317からステップ320へ移行する。

【0041】ブロック320でMSC30はUIM-IMEIロック機能が作動可能（イネーブル）になっているか否か判定する。この機能が作動可能であるか否か判定するための条件は、取り締まり問題やオペレータの好みやその他の要素に依存して大いに多様であり、従ってこの機能については「標準」動作モードは期待できなくて、全くオペレータの好みによる。しかし、この機能が作動可能であるならば、制御の流れはブロック320からブロック325へ分岐する。この機能が作動不能になっているならば制御の流れはブロック320からブロッ

ク330へ分岐する。
【0042】ブロック325において、MSC30は、UIM-IMEIロックコマンドを意味する保障要求を作成して、このメッセージをMT10へ送る。MT-UIMロックコマンドと同じく、UIM-IMEIロックコマンドは、UIM20に付随するAuC36の機能からのRAND及びSRES（真実性確認パラメータ）の対を、動作が本物である（真実性がある）ことを証明するための手段として含んでいる。ブロック325からブ

ロック330へ移行する。
【0043】MSC30の制御はステップ325からステップ326（図4及び図5参照）へ移行し、ここでMSC30は実際上、応答を待つか、或いはMT10のための応答を待ちながら時間切れとなるので、今や図4及び図5に示されているMT10の処理に焦点を合わせる。

【0044】前述したように、MT10がMSC30からメッセージを受け取ると、ステップ100から105までの制御が行われる。もしステップ105において、受け取られたメッセージがMT-UIMロックコマンドを意味するものでなかったならば、ステップ105から

ステップ110へ移行する。
【0045】ステップ110は、受け取ったメッセージの内容を検査して、それがUIM-IMEIロックコマンドを含んでいるか否か判定する。もし含んでいるならば、ステップ110からステップ125へ分岐する。もし含んでいなければ、ステップ110からステップ115へ分岐する。

【0046】ステップ115は、本発明には関係のないMSC30から受け取られた他のコマンドの処理を表しており、従って本発明の範囲内での処理は終了したと考えてよい。

【0047】ステップ125は、受け取られたUIM-IMEIロックコマンドが本物である（真実性がある）ことを保証するためのものである。図7（A）に示されているように、UIM-IMEIロックコマンドを意味する保障要求は、当該UIM20に付随するAuC36により該UIM20のために計算されたRAND及びSRESを含んでいる。図4のステップ120に関して前述したように、好ましい実施例では、MT10によりR

ANDに追加の強化要件が課される。それらの強化要件は実施者の決定により、ステップ120で選ばれたものと意図的に異ならしめることもできるし、同一であってもよい。もし強化されたRAND要件が承認されなければ、MT10はステップ135でそのコマンドは無効であると宣言してステップ136へ分岐する。そうでない場合にはUIM-IMEIロックコマンドはMT10からUIM20に渡され、更なる処理のためにMSC30から受け取られたメッセージに含まれるRAND及びSRESの両方を完備している。次にステップ135からステップ145へ移行する。

【0048】ステップ145において、MT10はUIM-IMEIロックメッセージをUIM20に送り、動作の結果又は時間切れを待つ。

【0049】図6は、UIM-IMEIロックコマンドの処理のためのUIM20内での制御の流れを示す。MT10のステップ145からのUIM-IMEIロックコマンドの受け取りでプロセスが始まり、その結果として図6のUIM20のステップ200となる。ステップ200からステップ205へ移行して、このステップでUIMは、UIM-IMEIロックメッセージに含まれているRANDを抽出して、通常の方法でSRESを計算する。ステップ205でUIM20がSRESを計算した後、ステップ210へ移行し、ここでUIM20により計算されたSRESと、MSC30からのUIM-IMEIロックメッセージに含まれているSRESとが比較される。その2つのSRESの値が同一であれば、ステップ210からステップ215へ分岐する。その2つのSRESの値が同一でなければ、ステップ210からステップ230へ移行する。

【0050】ステップ215においてUIM20はMT10からIMEI15を要求する。IMEI15の値は、将来、各初期化サイクルなどの際に参照するためにUIM20に記憶される。ステップ215からステップ220へ移行し、ここでステップ215の成功が検査される。もし動作が首尾よく終了すれば、ステップ220からステップ225へ移行する。もしそうでなければ、ステップ220からステップ230へ分岐する。

【0051】ステップ225は、UIMが今や首尾よく特定のIMEI15にロックされているという事実のインジケータをUIM20に記憶させることにより、その事実を記憶する。また、UIM20は、UIM-IMEIロックコマンドが首尾よく実行されたことをMT10に知らせる。ステップ225からステップ235へ移行してプロセスは終了する。

【0052】ステップ230は、ステップ145のUIM-IMEIロック動作の実行（又は時間切れ）の知らせをMT10に送り、ステップ146に進み、ここでもし動作が成功であったならば、MT10はステップ146からステップ147へ分岐する。もしそうでなけれ

ば、ステップ146からステップ136へ分岐する。

【0053】ステップ147において、MT10は、UIM-IMEIロックが成功したことを意味する保障応答 (SECURITY RESPONSE) を作成して、このメッセージをMSC30に送る。MT10の制御はステップ147からステップ150へ移行し、MT10のプロセスは終了する。

【0054】ステップ136においてMT10はUIM-IMEIロックの失敗を意味する保障応答を作成して、このメッセージをMSC30に送る。次にMT10の制御はステップ136からステップ150に移行し、MT10のプロセスは終了する。

【0055】ここで図3を参照すると、MSC30がMT10から応答を受け取るとステップ326からの制御の流れはステップ327へ進む。ステップ327においてMSC30は、ステップ330での参照のためにMT10から通知された結果を記憶する。次にステップ327からステップ330へ移行する。

【0056】ブロック330は管理に関する報告の処理をする。好ましい実施例では、その報告には、当該MT10のIMEI15、EIR60からのIMEI15に関連する状況、MT10に内蔵されているUIM20に関連するユーザーと、MSC30がとった行動とに関する情報と（これには、分岐の仕方により、報告のみ (Report Only)、MT-UIMロック (成功/失敗/試行されず)、UIM-IMEIロック (成功/失敗/試行されず) を含むことがある)、該当する場合にはMT10のロック動作の結果とが含まれる。これらの報告は、結局、将来行われるかも知れない犯罪調査等のために当該当局に送られる。

【0057】ここで図8を参照すると、ステップ605において、UIM20は現在のMT10のIMEI15を要求する。ステップ605からステップ610へ移行し、ここでステップ605のIMEI照会動作の成功が検査される。現在のMT10のIMEI15が受け取られると、ステップ610からステップ615へ分岐する。そうでない場合にはステップ605からステップ625へ分岐する。

【0058】ステップ615は、現在のMT10から受け取られたIMEI15と、図6のステップ215においてUIM20に記憶されたIMEI15とを比較する。もしその2つのIMEIの値が同一であれば、ステップ620からステップ699へ移行し、ここで通常の処理が継続され、本発明に関するプロセスは終了する。もしその2つのIMEIの値が同一でなければ、ステップ620からステップ625へ分岐する。

【0059】ステップ625において、UIM20は現在のMT10から受け取ったIMEI15とは異なるIMEI15に現在ロックされているために初期化プロセスが止められていることをMT10に知らせる。次にス

テップ625からステップ630へ移行してプロセスは終了する。

【0060】図7 (A) は、MSC30からMT10への保障要求メッセージの好ましい実施例である。このメッセージは新しいものであるが、このメッセージの幾つかの構成要素は既存のシステムに普通に使われているものである。新しい情報要素は保障要求メッセージタイプであり、これはメッセージのモビリティ管理セットの中でのこのメッセージタイプを一義的に特定する8ビットの値である。この値は標準化機構により割り当てられるものであり、モビリティ管理メッセージタイプの保障メッセージ範囲内で唯一無二の値であればどのような値でもよい。次の新しい情報要素は保障要求のタイプである。この情報要素の好ましい長さは8ビットである。1ビットは留保される。1ビットは要求されたロック状態を示すために使われ、0は「ロック解除」を意味し、1は「ロック」を意味する。1ビットは、MT-UIMロックを示し、1ビットはUIM-IMEIロックを示す。残りは留保される。MSC30が1つのメッセージを介してMT10にロック動作をすること又は両ロックをロック解除することを指令するように、このMT-UIMビット及びUIM-IMEIビットをビットマスクとして使用することができる。しかし、好ましい実施例は、簡単のために、メッセージ毎に1回のロックだけである。本発明を実施するために他の多くのフォーマット及び構造を採用することができる。

【0061】図7 (B) はMT10からMSC30への保障応答の好ましい実施例である。図7 (A) に記されているように幾つかの情報要素は従来から使われているものである。保障応答メッセージタイプは、メッセージのモビリティ管理セットの中でのこのメッセージタイプを一義的に特定する8ビットの値である。この値は標準化機構により割り当てられるものであり、モビリティ管理メッセージタイプの保障メッセージ範囲内で唯一無二の値であればどのような値でもよい。保障要求のタイプは図7 (A) に記載されているとおりである。簡単のために、好ましい実施例はメッセージ毎に1回のロック動作だけである。しかし、保障応答メッセージ中に2個以上のロック識別子セットがあるならば、各ロック識別子セットにつき1個ずつ、合計で複数の結果コード情報要素があることになる (即ち、値1)。結果コードは、第1結果コードIEIがロッキングビットマップの最下位ビットで特定されるロック等に対応することとなるようにマッピングする。「0」という値は動作が成功したことを意味する。「1」という結果コードの値は、UIM20により計算されたSRESが保障要求の中のSRESと一致しなかったので失敗であったことを意味する。「10」という2進法の結果コードは真実性の確認要求メッセージをMSC30に送る好ましい強化方法の時間切れ失敗により動作が失敗したことを意味する。「1

1」という2進法の結果コードは、MSC30からの真実性の確認応答のSRESが正しくなかったことを意味する。他の全ての値は種々のタイプの失敗を表し、その意味を知っているのは当該MT10の製造者だけである。本発明を実施するために他の多くのフォーマット及び構造を採用することができる。

【0062】図8は、本発明のUIM-IMEIロックを実現するために在来の論理より前に挿入しなければならないUIM20の論理を示す。ステップ600において、UIM20の従来から行われている種類の処理の際になるべく早く、且つUIM20の初期化が完了する前に、UIM20はその制御構造をチェックして、現在UIM20が特定のMT10に付随する特定のIMEI15にロックされているか否かを判定する。もしそうであれば、ステップ600からステップ605へ分岐する。もしそうでなければ、ステップ600からステップ699へ分岐して、ここで従来から行われている種類の処理が継続され、本発明に関連する処理は終了する。

【0063】移動端末装置MT10の初期化処理のための類似の形を設けることができるけれども、MT10からUIM20へのロッキングは現在は種々の起動方法を介して行われているので、この情報は当業者に周知されていて、ここでは説明しない。

【0064】メッセージを介してMT-UIM機能及びUIM-IMEI機能の両方のロック解除を支援することも本発明の目的である。当業者のために、保障要求メッセージのフォーマットは、図7(A)に関して説明した「ロック解除」ビットを介してこれを支援する。ロック解除動作のための論理及び制御の流れは図4乃至図6を考察すれば明かである。MSC30についての論理的ロック解除動作は、トリガーを除けば図2及び図3のロック動作と全く同じである。ステップ310は、以前はブラックリストに載せられていたMT10のホワイトリストへの記入、又は適当なロック解除コマンドを強制的に送らせるためのオペレータの専門技術者及び種々のMSC30インターフェースを介しての手操作による対話であってもよい。好ましい実施例は、「ブラックリス

ト」から「ホワイトリスト」への「バッチ」型転載処理と手操作による介入との両方を支援する。

【0065】本発明の好ましい実施例を詳しく開示したけれども、明細書に記載の特許請求の範囲の欄において定義した発明の範囲から逸脱せずに、説明をした実施例について種々の変更がされ得ることを当業者は理解すべきである。

【図面の簡単な説明】

【図1】本発明の通信網の1実施例を示す略ブロック図である。

【図2】本発明の方法によるメッセージの処理のための通信網論理(図1のMSC30)のフローチャート(その1)である。

【図3】本発明の方法によるメッセージの処理のための通信網論理(図1のMSC30)のフローチャート(その2)である。

【図4】本発明の方法によるメッセージの処理のための移動端末装置論理(図1のMT10)のフローチャート(その1)である。

【図5】本発明の方法によるメッセージの処理のための移動端末装置論理(図1のMT10)のフローチャート(その2)である。

【図6】本発明で取り入れたメッセージの処理のためのユーザー識別モジュール論理(図1のUIM20)のフローチャートである。

【図7】(A)および(B)はそれぞれ、本発明に用いることのできるメッセージの構成を示す。

【図8】本発明の実施例におけるUIM-IMEIロックを実行するために図1のUIM20において必要とされる初期化論理についてのフローチャートである。

【符号の説明】

MT…移動端末装置

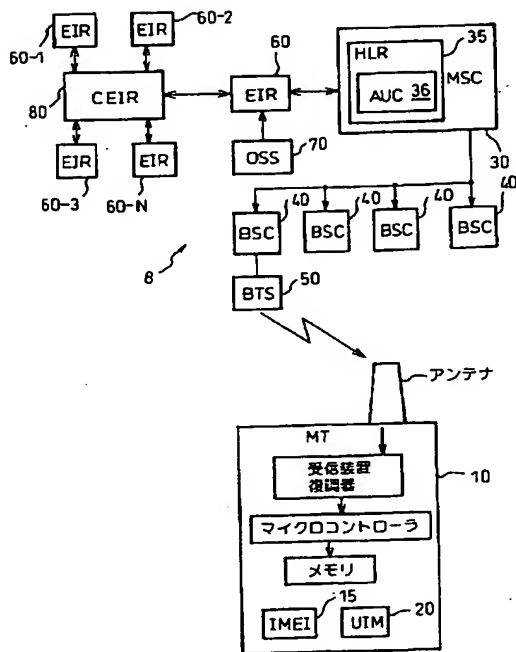
UIM…ユーザー識別モジュール

IMEI…国際移動端末装置識別ユニット

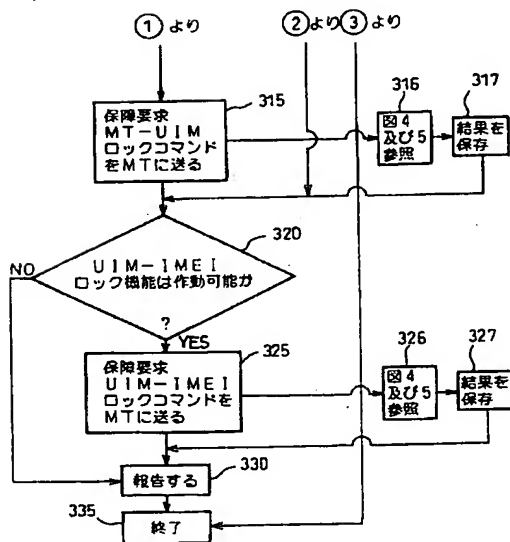
MSC…移動交換センター

BSC…基地局コントローラ

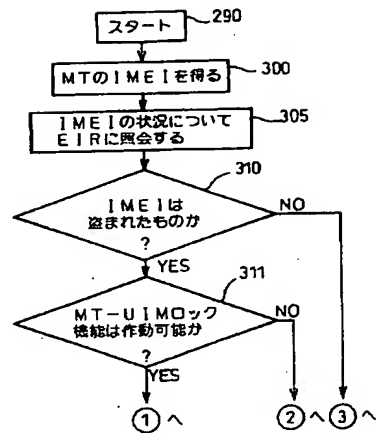
【図1】



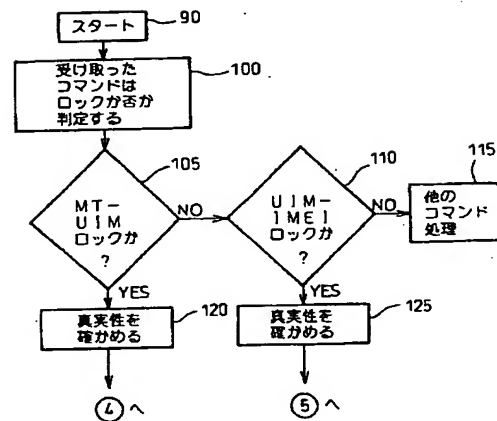
【図3】



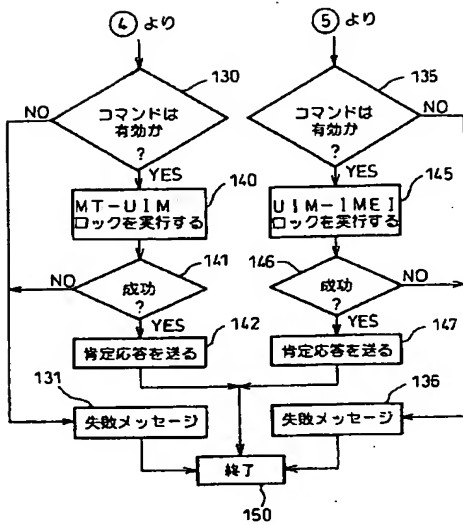
【図2】



【図4】



【図5】



【図7】

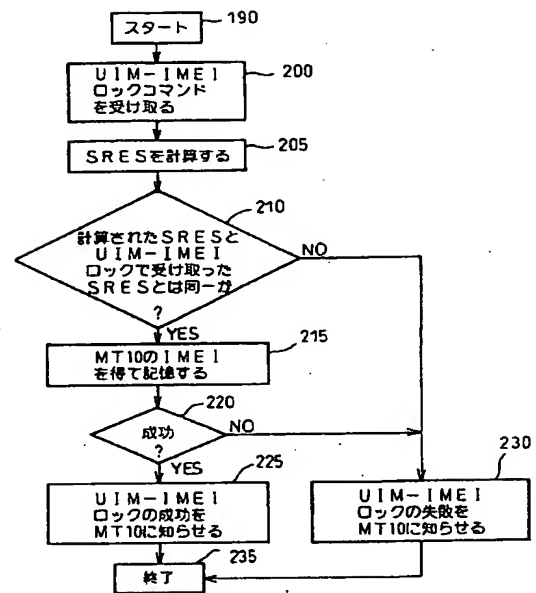
(A) 保障要求

モビリティ管理プロトコルディスクリミネータ
スキップインジケータ
保障要求メッセージタイプ
保障信号のタイプ
真実性パラメータRAND
真実性パラメータSRES

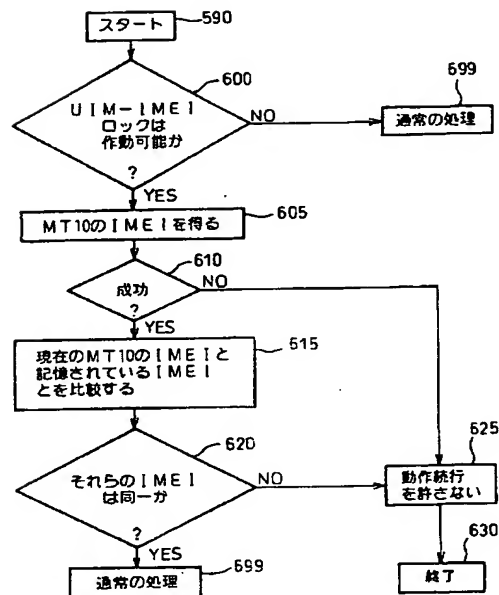
(B) 保障応答

モビリティ管理プロトコルディスクリミネータ
スキップインジケータ
保障応答メッセージタイプ
保障要求のタイプ
結果コード

【図6】



【図8】



【手続補正書】

【提出日】平成8年8月14日

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】請求項9

【補正方法】変更

【補正内容】

【請求項9】 前記移動交換センター（MSC）は、真実性の確認センター（AuC）を有するホームロケーション・レジスタ（HLR）を含んでおり、前記移動交換センター（MSC）は、前記移動端末装置の正当性及び状況に関するデータを内蔵する装置識別レジスタ（EIR）に接続されている、請求項8に記載の移動通信網。

【手続補正2】

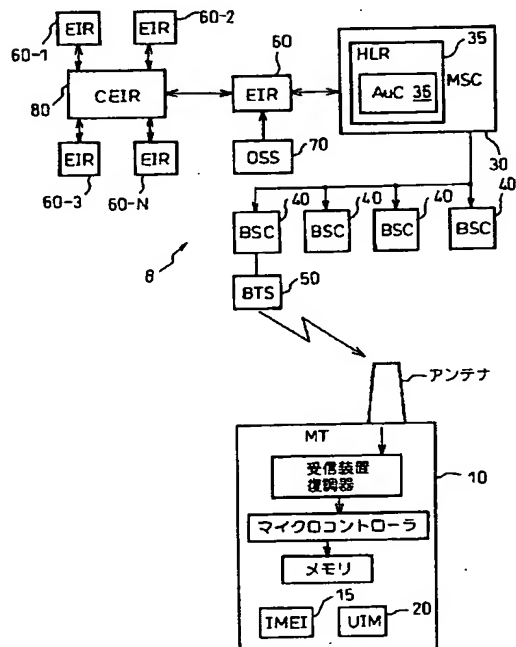
【補正対象書類名】図面

【補正対象項目名】図1

【補正方法】変更

【補正内容】

【図1】



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☒ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.